Corrigé du DS n°1 : arithmétique

Vrai-Faux

1) La première affirmation est bien évidemment fausse : il existe bien des couples d'entiers (q, r) tel que $a = bq + r$, mais l'unicité de ce couple n'est assuré que par une hypothèse supplémentaire : $0 \leqslant r < |b|$.

2) La deuxième affirmation est encore fausse : $a \equiv b \pmod 8$ implique bien $a^2 \equiv b^2 \pmod 8$ (compatibilité des relations de congruence avec les puissances), mais la réciproque est fausse : $4 \not\equiv 8 \pmod 8$, et pourtant $4^2 \equiv 8^2 \pmod 8$.

3) $10^2 = 100 = 6 \times 15 + 10 \equiv 10 \pmod{15}$, donc par récurrence, $10^n \equiv 10 \pmod{15}$ pour tout $n \in \mathbb{N}^*$. En particulier, le reste de la division euclidienne de 10^{2006} par 15 est 10.

4) Un entier compris entre 0 et 9999 s'écrit avec 4 chiffres compris entre 0 et 9. Si on écrit tous ces nombres en colonne, chaque chiffre apparaît dans chaque colonne autant de fois. Il y a donc 1000 chiffres 4 dans chaque colonne, d'où 4000 chiffres 4 en tout (le nombre 10000 ne rajoute pas de nouveu chiffre 4 !).

5) Pour trouver le nombre de 0 par lequel se termine l'entier 100!, il suffit de compter le nombre de facteurs 5 dans les entiers compris entre 1 et 100.

   Il y a 20 multiples de 5 entre 1 et 100, dont 4 multiples de 25. Il y a suffisamment de multiples de 2 entre 1 et 100 pour faire autant de multiples de 10. Il y a donc donc $20 + 4 = 24$ chiffres 0 au bout de l'écriture décimale de 100!.

Restitution organisée de connaissances, et application

1) **Démonstration de cours**

   (a) Démontrons maintenant la première relation. Notons $\mathscr{P}_n$ la propriété : $a^n \equiv b^n \pmod m$.
   L'hypothèse $a \equiv b \pmod m$ dit exactement que $\mathscr{P}_1$ est vraie.
   Supposons $\mathscr{P}_n$ vraie pour un certain entier n. Alors $a^n \equiv b^n \pmod m$. De $a \equiv b \bmod (m)$ et du deuxième prérequis, on déduit :

$$a^{n+1} = a^n.a \equiv b^n.b = b^{n+1} \pmod m$$

   Ainsi, $\mathscr{P}_{n+1}$ est encore vraie.
   $\mathscr{P}_n$ est donc héréditaire, et par le principe de récurrence, $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}^*$.

2) **Exercice**

   (a) Écrivons les restes des carrés modulo 3, puis les restes modulo 7 des puissances sixièmes (on commence par calculer $n^3 \pmod 7$, puis on élève ce reste au carré) :

$n \pmod 3$	0	1	2
$n^2 \pmod 3$	0	1	1

$n \pmod 7$	0	1	2	3	4	5	6
$n^3 \pmod 7$	0	1	1	6	1	6	6
$n^6 \pmod 7$	0	1	1	1	1	1	1

   On a donc bien : $n^2 \equiv 1 \pmod 3$ et $n^6 \equiv 1 \pmod 7$ si n n'est ni un multiple de 3, ni un multiple de 7.
   On a donc :

$$n^{37} = n^{3*12+1} = \left(n^3\right)^{12}.n \equiv n \pmod 3$$

   et de même

$$n^{37} = n^{6*6+1} = \left(n^6\right)^{6}.n \equiv n \pmod 7$$

   (b) Reste à appliquer ce qui précède au numérateur de la fraction $\frac{10}{21}n^{37} + \frac{11}{21}n$:

$$10n^{37} + 11n \equiv 10n + 11n \equiv 21n \equiv 0 \pmod{3 \text{ ou } 7}$$

   $10n^{37} + 11n$ est donc divisible par 3 et 7, donc par 21.

Exercice 1

1) $u_1 = 64$, $u_2 = 314$, $u_3 = 1564$, $u_4 = 7\,814$. On remarque que les deux derniers chiffres de u_n ont l'air d'alterner entre 14 et 64.

   Cela est confirmé par l'observation de $u_5 = 39\,064$ et $u_6 = 195\,314$.

2) (a) $u_{n+2} = 5u_{n+1} - 6 = 5\,(5u_n - 6) - 6 = 25u_n - 36$. Comme $25 \equiv 1\,(\bmod 4)$ et $36 \equiv 0\,(\bmod 4)$, on a donc $u_{n+2} \equiv u_n\,(\bmod 4)$.

   (b) Les termes de rangs pairs de la suite (u_n) sont donc[1] congrus à u_0 modulo 4, soit à 2. Les termes de rangs impairs sont quant-à eux congrus à u_1 modulo 4, soit à 0.

3) (a) Notons $\mathscr{P}_n$ l'assertion : $2u_n = 5^{n+2} + 3$.
   $\mathscr{P}_0$ est clairement vraie : $5^{0+2} + 3 = 28 = 2 \times 14 = 2u_0$.
   Supposons $\mathscr{P}_n$ vraie pour un certain rang n. On a alors :

$$2u_{n+1} = 2\,(5u_n - 6) = 5.2u_n - 12 = 5^{n+3} + 15 - 12 = 5^{n+3} + 3$$

   donc $\mathscr{P}_{n+1}$ est encore vraie. L'assertion est donc vraie pour tout $n \in \mathbb{N}$.

   (b) Observons les puissances de 5 modulo 100 :

n	0	1	2	3	4 ...
$5^n\,(\bmod 100)$	1	5	25	25	25 ...

   On peut facilement démontrer (par une récurrence "évidente") que $5^n \equiv 25\,(\bmod 100)$ pour tout $n \geqslant 2$.
   Ainsi : $2u_n = 5^{n+2} + 3 \equiv 25 + 3 = 28\,(\bmod 100)$.

4) Il existe donc un entier N_n tel que $2u_n = 100N_n + 14$. Ainsi, $u_n = 50N_n + 14$. Les deux derniers chiffres de u_n sont donc 14 ou 64, selon que N_n est pair ou impair. Mais cela dépend en fait du reste de la division de u_n par 4. Ainsi :

$$u_{2p} = 100P_p + 14 \quad \text{et} \quad u_{2p+1} = 100Q_p + 64$$

Exercice 2

On se propose de démontrer, en raisonnant modulo 4, que l'équation $x^2 + 3y^2 = 942$ n'a pas de solution.

1) Voici les restes de n^2 et $3n^2$ modulo 4 :

$n\,(\bmod 4)$	0	1	2	3
$n^2\,(\bmod 4)$	0	1	0	1
$3n^2\,(\bmod 4)$	0	3	0	3

2) On peut construire une table réunissant tous les cas possibles. Il est plus simple de recenser simplement les différents restes possibles de $x^2 + 3y^2$: cela peut être $0 = 0 + 0 = 1 + 3$, $1 = 0 + 1 = 1 + 0$ ou $3 = 0 + 3$.

3) On vient de voir que le seul reste qu'on ne peut rencontrer est 2, or c'est précisément le reste de la division euclidienne de 942 par 4. Si l'équation $x^2+3y^2 = 942$ avait une solution (dans $\mathbb{Z}^2$), alors cette relation demeurerait modulo 4, ce qui est impossible.

   L'équation $x^2 + 3y^2 = 942$ n'a donc pas de solution.

[1] Une démonstration rigoureuse de ces deux résultats devrait faire intervenir une récurrence, dont le caractéère évident permet de se passer, la seule difficulté consistant à écrire l'hypothèse.